

# SCADA systems

# Introduction

- **SCADA :**

“Supervisory Control And Data Acquisition”

- A type of *Industrial Control System* (ICS) that is used to monitor & remotely control critical industrial processes.

# Why the emphasis on SCADA ?

- SCADA supports Critical Infrastructures of a nation e.g.
  - ✓ Electrical Power Grids
  - ✓ Oil & Gas pipelines
  - ✓ Refineries and chemical plants
  - ✓ Water and wastewater systems
  - ✓ Manufacturing operations

# SCADA components

## 1. Field Instrumentation

e.g. CT, PT, RTU, PLC

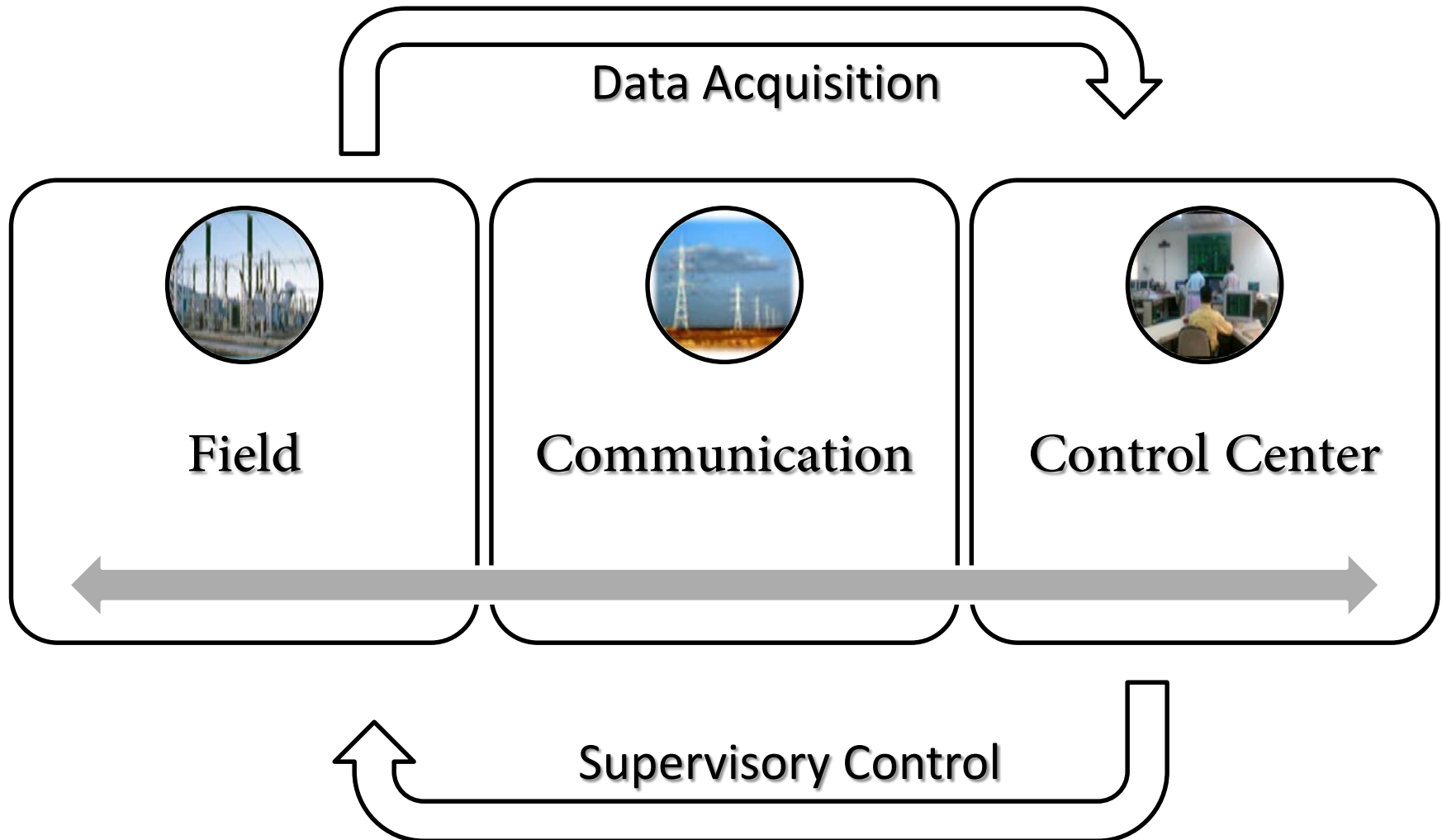
## 2. Communication Network

e.g. Cable, PLCC, Wideband, GPRS

## 3. Control Center

e.g. SLDC, Master SCADA

# SCADA components



# SCADA components

## [1].Field Instrumentation:

- Collects all info of the system & transport to the control center.
- Installed @ Field Station
- Collects info by CTs, PTs, Transducer, RTUs(Remote Terminal Unit), IEDs(Intelligent Electronic Devices)

# SCADA components

## [1].Field Instrumentation:

Types of info associated in a power system -

### Digital Information

- Breaker Status
- Isolator Status

### Analog Information

- Voltage
- Current
- Frequency
- Power Factor

# SCADA components

## [2]. Communication Network:

- Dedicated Telephone Lines
- PLCC (Power Line Carrier Communication)
- VHF (Very High Frequency)
- Microwave
- GPRS (General Pocket Radio Service)
- Optical Fibre



# SCADA components

## [3]. Control Centre:

- Front End System- Interface between RTU & master SCADA
- Data Base
- HMI (Human-Machine Interface)
- LAN
- Peripheral

# SCADA components

## [3]. Control Centre:

### Control Strategy : Key Priorities

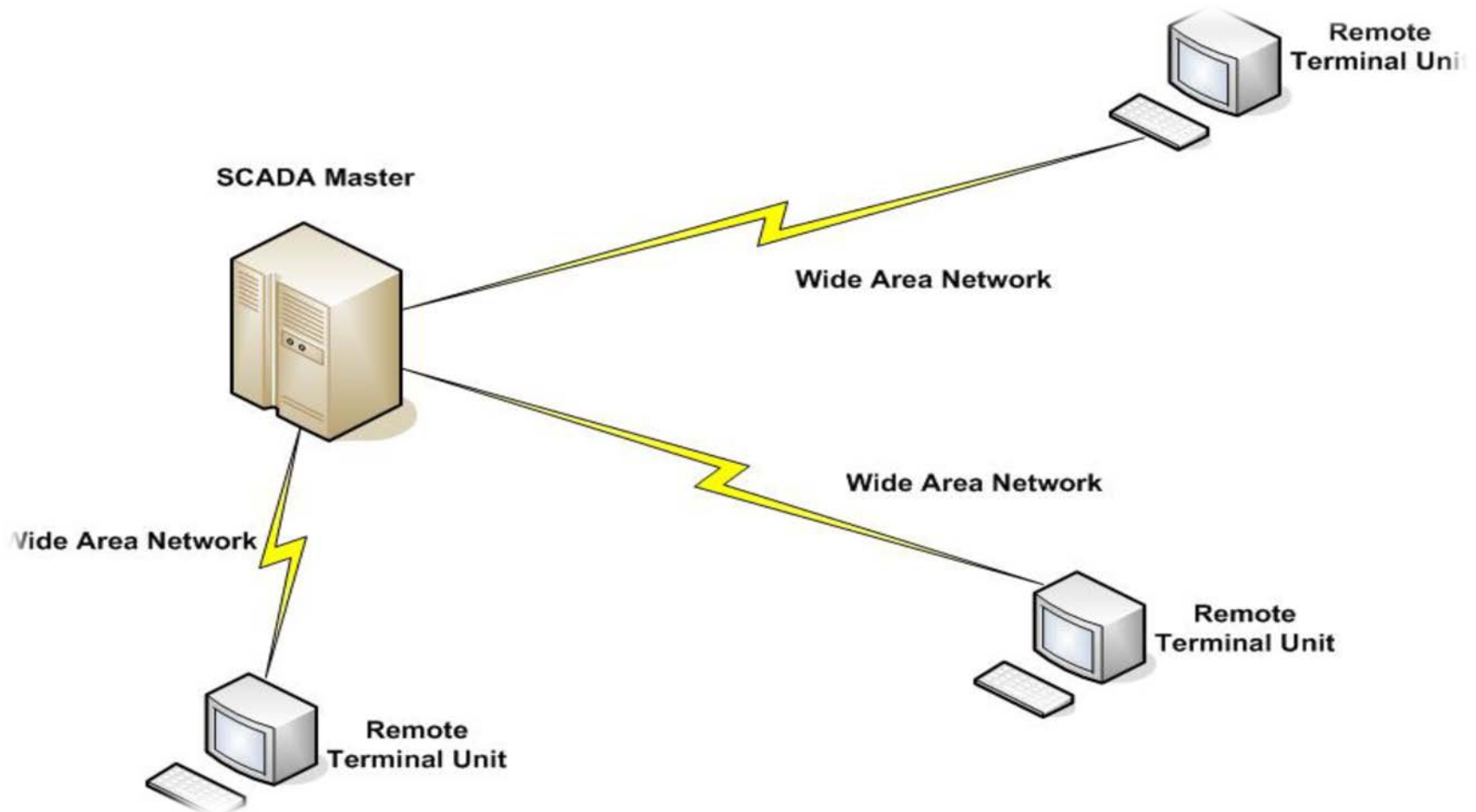
- Balance generation & demand (dispatching)
- Monitor flows and observe system limits
- Coordinate maintenance activities
- Protect equipment from damage

# SCADA architecture

- First Generation – Monolithic
- Second Generation – Distributed
- Third Generation – Networked

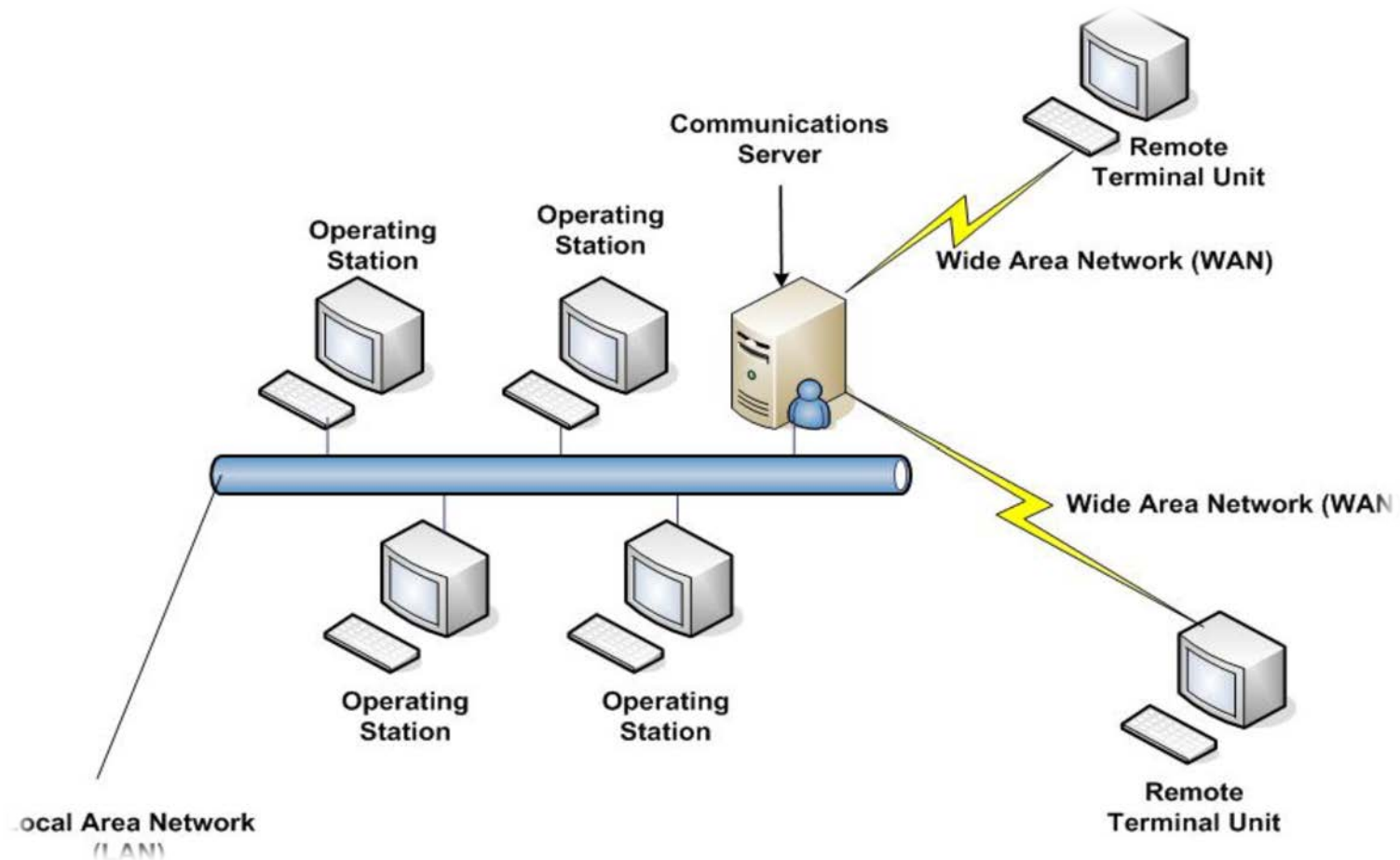
# SCADA architecture

## First Generation – Monolithic



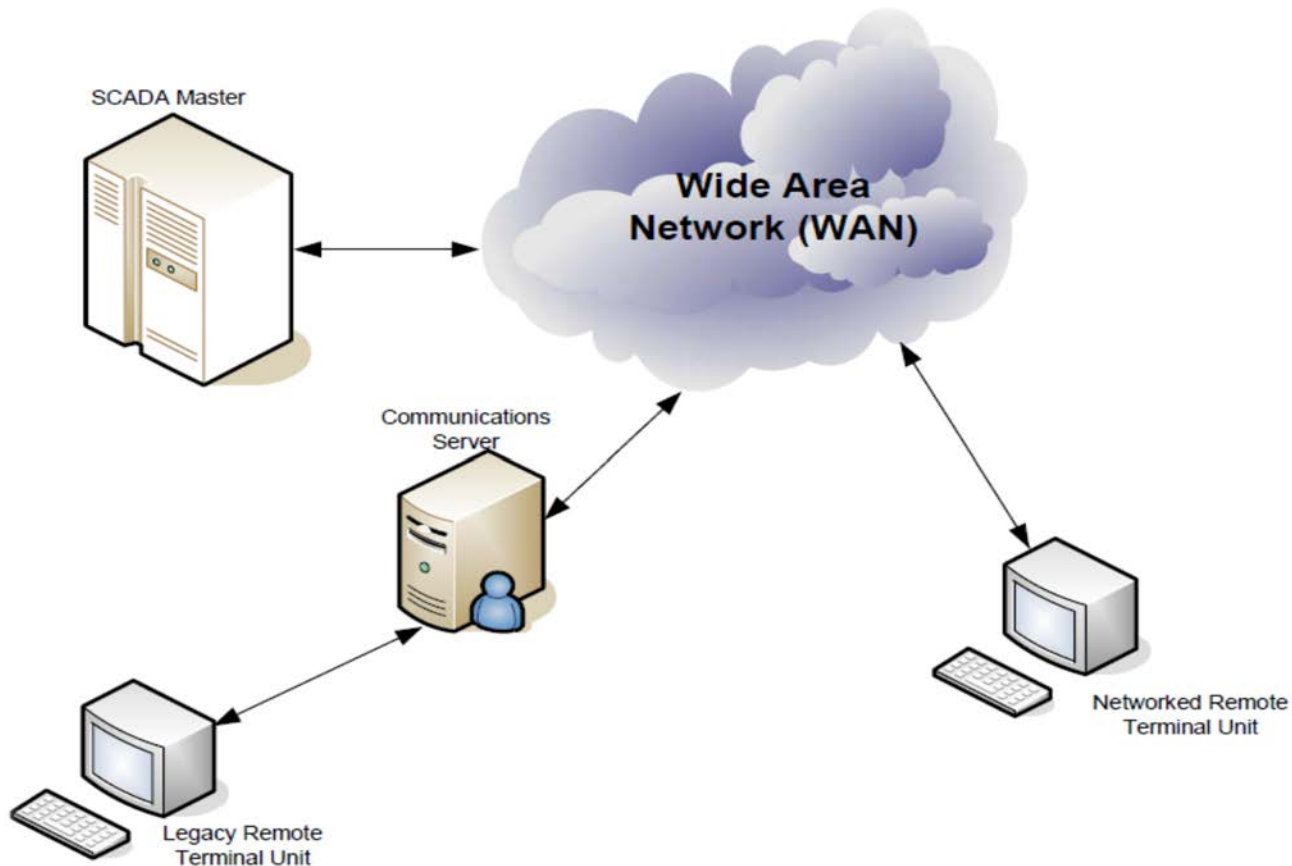
# SCADA architecture

## Second Generation – Distributed



# SCADA architecture

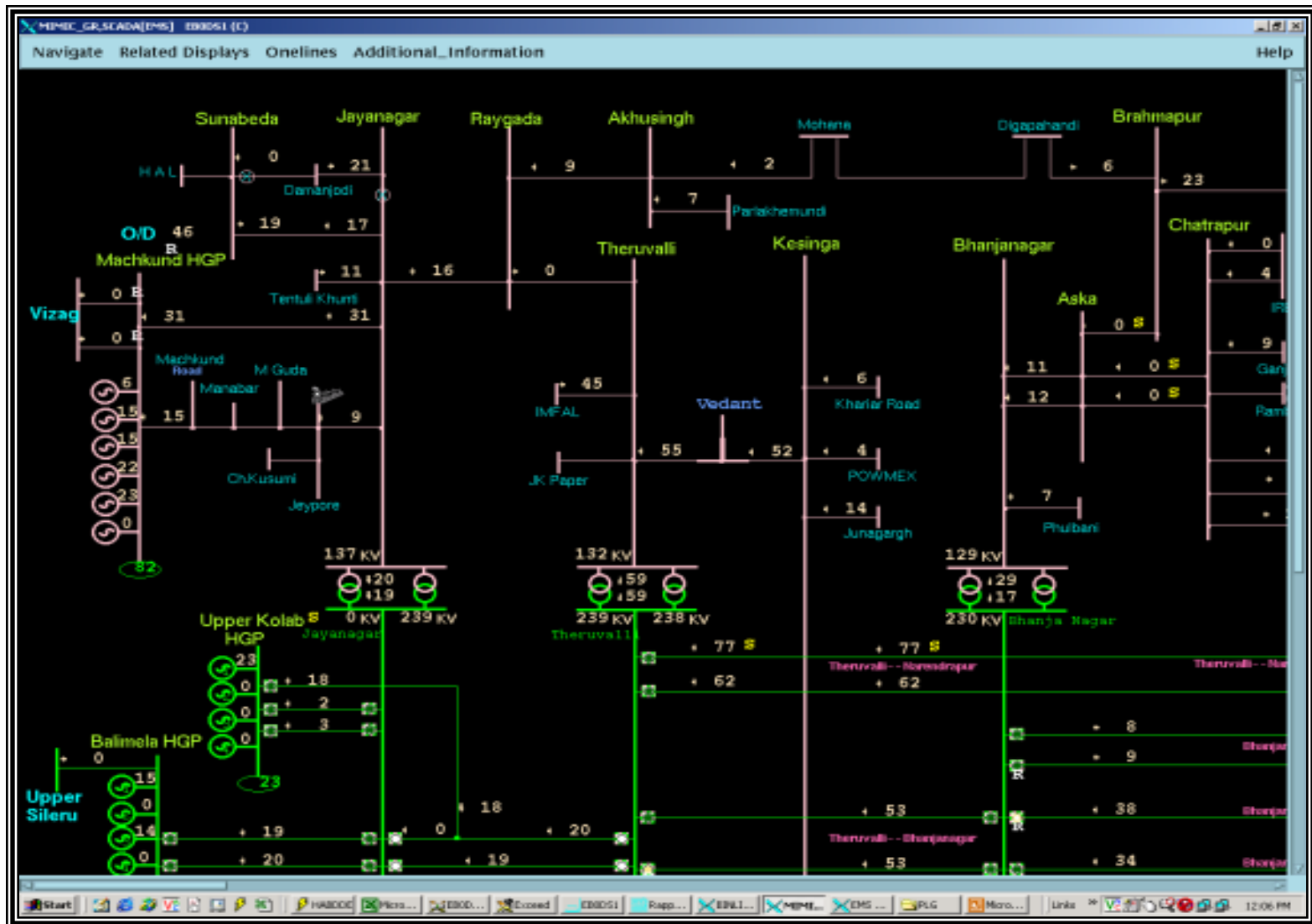
## Third Generation – Networked



# Functions of SCADA system

- Information Display
- Supervisory Control
- Alarm Processing & Tagging
- Information Storage & Reports
- Data Calculation
- Special RTU Processing Control

# Information Display





# Alarm Processing & Tagging

The screenshot displays the BLOC (BLOCK) software interface, which is used for monitoring and managing power system components. The main window shows a list of devices and their associated alarms, organized into columns for different system areas like 'BLOC', 'OPTO', 'MOTOR', and 'MOTOR'. The interface includes various status indicators (e.g., 'ON', 'OFF', 'ALARM') and a detailed view of the system's current state.

The screenshot displays the TAGLIST (TAGGING) software interface, which is used for managing tags and their associated data. The main window shows a list of tags, organized into columns for 'Substation', 'Device Type', 'Device', 'Point', and 'Tag Type'. The interface includes various status indicators (e.g., 'ON', 'OFF', 'ALARM') and a detailed view of the system's current state.

**Tag List Table:**

Substation	Device Type	Device	Point	Tag Type
BALIM GR	CB	E 04/H06	STTS	RED
BALIM GR	CB	E 10/JAYAN-3	STTS	REDFOR
NAREN GR	CB	E 04/THRU-1	STTS	RED
TARKE GR	CB	D 00/RSP _1	STTS	GREEN
TARKE GR	CB	D 00/RSP _1	STTS	GREEN
TARKE GR	CB	D 15/CHEND-2	STTS	GREEN

**Tag Information Window (TAGLIST-TAG\_LIST\_001):**

Substation: BALIM GR  
 Device: E 04/H06  
 Tag Type: RED  
 Hidden Number: 10  
 Placed In: 15-MAY-2006 13:52:20  
 Placed By: MANAGER.BALIM  
 Placed For: ANNUAL MAINT  
 Comments: SHUT DOWN FROM 02-05-2006 TO 01-06-2006

**Tag Information Window (TAGLIST-TAG\_LIST\_002):**

Substation: TARKE GR  
 Device: D 00/RSP \_1  
 Point: STTS  
 Tag Type: GREEN  
 Hidden Number: 10  
 Placed In: 31-MAY-2006 17:03:20  
 Placed By: MGR, TARKERA  
 Placed For: S/D  
 Comments: S/D OF 132KV TARKERA-RSP 1 FROM 7-17HRS ON 1ST JUNE 2006

# Information Storage & Reports

HDR\_SCADA [EMS] EB0DS1 (VIEWPORT\_1) Page:1

Navigate Related Displays Help

## Historical Data Recording SCADA

Recording Files... Present Status: Active

Disposition Message:

### RECORDING FILE DIRECTORY

Filename	Start Time	End Time	Status	To Be Deleted
HDR\$_EMPTY_2156_14_1.B01			Empty	<input type="checkbox"/>
HDR_070910_2156_11_0.B01	10-SEP-2007 21:56:11	10-SEP-2007 22:05:23	Recording	
HDR_070910_2144_44_8.B01	10-SEP-2007 21:44:44	10-SEP-2007 21:56:09	Backed Up	<input type="checkbox"/>
HDR_070910_2133_18_6.B01	10-SEP-2007 21:33:18	10-SEP-2007 21:44:42	Backed Up	<input type="checkbox"/>
HDR_070910_2121_54_4.B01	10-SEP-2007 21:21:54	10-SEP-2007 21:33:16	Backed Up	<input type="checkbox"/>
HDR_070910_2111_19_2.B01	10-SEP-2007 21:11:19	10-SEP-2007 21:21:52	Backed Up	<input type="checkbox"/>
HDR_070910_2100_01_0.B01	10-SEP-2007 21:00:01	10-SEP-2007 21:11:17	Backed Up	<input type="checkbox"/>
HDR_070910_2048_25_8.B01	10-SEP-2007 20:48:25	10-SEP-2007 20:59:59	Backed Up	<input type="checkbox"/>
HDR_070910_2036_56_6.B01	10-SEP-2007 20:36:56	10-SEP-2007 20:48:23	Backed Up	<input type="checkbox"/>
HDR_070910_2025_48_4.B01	10-SEP-2007 20:25:48	10-SEP-2007 20:36:54	Backed Up	<input type="checkbox"/>
HDR_070910_2014_38_2.B01	10-SEP-2007 20:14:38	10-SEP-2007 20:25:46	Backed Up	<input type="checkbox"/>
HDR_070910_2003_39_0.B01	10-SEP-2007 20:03:39	10-SEP-2007 20:14:36	Backed Up	<input type="checkbox"/>
HDR_070910_1952_31_8.B01	10-SEP-2007 19:52:31	10-SEP-2007 20:03:37	Backed Up	<input type="checkbox"/>
HDR_070910_1941_30_6.B01	10-SEP-2007 19:41:30	10-SEP-2007 19:52:29	Backed Up	<input type="checkbox"/>
HDR_070910_1930_02_4.B01	10-SEP-2007 19:30:02	10-SEP-2007 19:41:28	Backed Up	<input type="checkbox"/>
HDR_070910_1918_30_2.B01	10-SEP-2007 19:18:30	10-SEP-2007 19:30:00	Backed Up	<input type="checkbox"/>
HDR_070910_1907_45_0.B01	10-SEP-2007 19:07:45	10-SEP-2007 19:18:28	Backed Up	<input type="checkbox"/>
HDR_070910_1856_55_8.B01	10-SEP-2007 18:56:55	10-SEP-2007 19:07:43	Backed Up	<input type="checkbox"/>
HDR_070910_1845_00_6.B01	10-SEP-2007 18:45:00	10-SEP-2007 18:56:53	Backed Up	<input type="checkbox"/>
HDR_070910_1833_28_4.B01	10-SEP-2007 18:33:28	10-SEP-2007 18:44:58	Backed Up	<input type="checkbox"/>
HDR_070910_1822_19_2.B01	10-SEP-2007 18:22:19	10-SEP-2007 18:33:26	Backed Up	<input type="checkbox"/>
HDR_070910_1811_47_0.B01	10-SEP-2007 18:11:47	10-SEP-2007 18:22:17	Backed Up	<input type="checkbox"/>
HDR_070910_1800_43_8.B01	10-SEP-2007 18:00:43	10-SEP-2007 18:11:45	Backed Up	<input type="checkbox"/>
HDR_070910_1741_14_6.B01	10-SEP-2007 17:41:14	10-SEP-2007 18:00:41	Backed Up	<input type="checkbox"/>
HDR_070910_1729_58_4.B01	10-SEP-2007 17:29:58	10-SEP-2007 17:41:12	Backed Up	<input type="checkbox"/>
HDR_070910_1718_15_2.B01	10-SEP-2007 17:18:15	10-SEP-2007 17:29:56	Backed Up	<input type="checkbox"/>
HDR_070910_1707_21_0.B01	10-SEP-2007 17:07:21	10-SEP-2007 17:18:13	Backed Up	<input type="checkbox"/>
HDR_070910_1656_14_8.B01	10-SEP-2007 16:56:14	10-SEP-2007 17:07:18	Backed Up	<input type="checkbox"/>

Start | VirusSca... | NPLG | GRIDCO... | ER-ULD... | PC RAP... | Exceed | RFGHelp | Rapport... | HDR,S... | Rtrapp... | 10:05 PM

# Data Calculation

GENCALC\_OPERATIONS.GENCALC(MS) L00051 (MILWY001\_1) page:3

Navigate Related Displays

Generalized Calculations Operations

Insert First Generalized Calculation

Select this button to insert New Calculation or Delete Calculation

Function: **NEW UI** Status: Enabled Creation time: 10-AUG-2007 16:09:42

Period: **2**

Start: **27-APR-2007 16:17:16**

Stop: **27-APR-2008 16:17:16**

Next run time: 09-SEP-2007 19:31:30

USERCALC task link status: Valid

Link file creation time: 10-SEP-2007 08:59:01

Process Calculation...

Activate Calculation...

Workarea for Generalized Function

Select box to insert first Formula Record

Generalized Function ID	Type	Out	Index	Substa
IF(FREQ.LE.40.0)THEN	PAISA	Analog	207.64	REPOT_GR
PAISA-745	FR3Q	Analog	3542	BIDAN_GR
ELSEIF(FREQ.LE.40.5)THEN				
PAISA-745 INT(FREQ 40.5/50)*16				
ELSEIF(FREQ.LE.40.8)THEN				
PAISA-345 INT(FREQ 40.5/50)*9				
ELSEIF(FREQ.LE.50.5)THEN				
PAISA-210 INT(FREQ 40.8/50)*6				
ELSE				
PAISA-4				
ENDIF				

GENCALC\_OPERATIONS.GENCALC(MS) L00051 (C) page:11

Navigate Related Displays

Generalized Calculations Operations

GENCALC

Insert First Generalized Calculation

Select this button to insert New Calculation or Delete Calculation

Function: **NEW UI** Status: Enabled Creation time: 10-AUG-2007 16:09:42

Period: **2**

Start: **27-APR-2007 16:17:16**

Stop: **27-APR-2008 16:17:16**

Next run time: 09-SEP-2007 19:31:30

USERCALC task link status: Valid

Link file creation time: 10-SEP-2007 08:59:01

Process Calculation...

Activate Calculation...

Workarea for Generalized Function

Select box to insert first Input / Output Record

Generalized Function ID	Type	Out	Index	Substa
IF(FREQ.LE.40.0)THEN	PAISA	Analog	207.64	REPOT_GR
PAISA-745	FR3Q	Analog	3542	BIDAN_GR
ELSEIF(FREQ.LE.40.5)THEN				
PAISA-745 INT(FREQ 40.5/50)*16				
ELSEIF(FREQ.LE.40.8)THEN				
PAISA-345 INT(FREQ 40.5/50)*9				
ELSEIF(FREQ.LE.50.5)THEN				
PAISA-210 INT(FREQ 40.8/50)*6				
ELSE				
PAISA-4				
ENDIF				

# Problems with SCADA

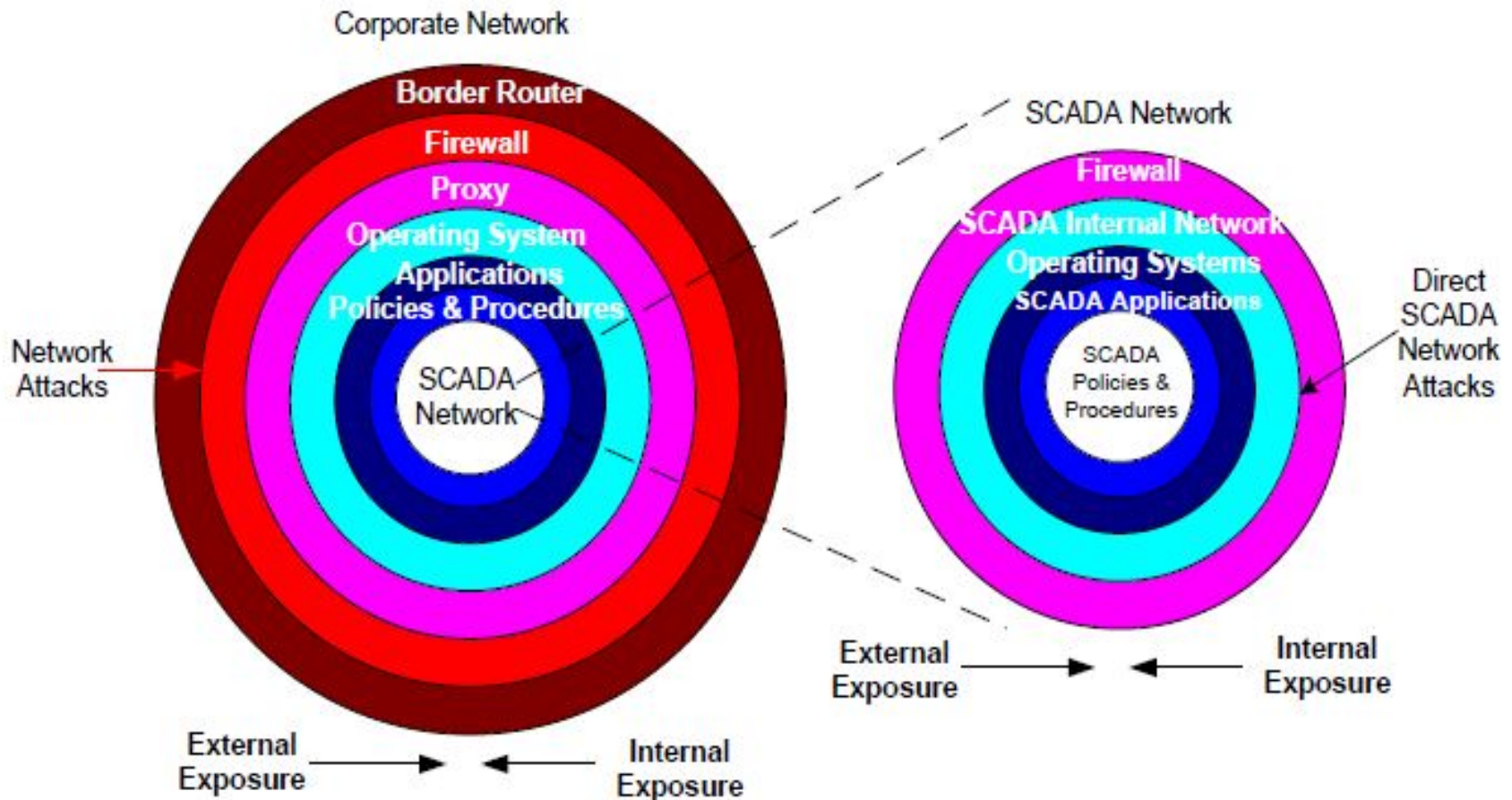
- No authentication (Unencrypted Communication)
- No security patching
- Multiple access points
- Complex System
- Dependent on industries driven by profit, not security

# Mitigation Strategy

- Security through obscurity
  - Poor defence against “structured adversary”
- Isolated network
  - Unrealistic given today’s business demands
- Communication encryption
  - Concerns over latency, reliability
- Signal authentication
  - May provide good defence without the concerns associated with full signal encryption



# Ring of Defenses



# Steps for Enhancing SCADA security

- Establish a robust network architecture.
- Eliminate untrusted remote access points of entry.
- Evaluate and deploy technology and approaches to enhance confidentiality, availability, and integrity.
- Provide adequate support and training
- Never become complacent !! 😊

# Last Words...

SCADA systems are becoming more & more interconnected and more accessible to the same villains who attacks our IT networks. But the difference is comparable: losing e-mail is not the same as millions of gallons of water from a reservoir or an electrical blackout !!!



**Thank You& Have a Good  
Time...**